一种改进的 R-LWE 同态掩码方案 *

李子臣 [1,2]，孙亚飞 [1]，杨亚涛 [1,3]，梁　斓 [1]，曹广灿 [3]

(1. 西安电子科技大学 通信工程学院，西安 710071; 2. 北京印刷学院，北京 102600; 3. 北京电子科技学院，北京 100070)

摘　要： 针对格上加密方案的差分能量攻击，Reparaz 等人在 PQC 2016 上提出一种具有加法同态的 R-LWE 掩码方案。该方案能够有效的抵抗差分能量攻击，但由于密文的同态加法造成密文中噪声尺寸增大，降低解密正确率。针对这一问题，提出一个改进的 R-LWE 同态掩码方案。引入模转换技术，对同态加密之后的密文进行模规约，在保证明密文对应的前提下，降低密文中的噪声尺寸，提高方案的解密正确率。为了保护子密钥，引入随机矩阵对子密钥进行掩码保护，并给出正确性分析及安全性证明。分析表明，相对于原方案，新方案从安全性和效率上都有较大的提升。

关键词： 格密码；R-LWE；侧信道攻击防御；掩码矩阵；模数转换；同态

中图分类号： TP　　doi: 10.3969/j.issn.1001-3695.2017.07.0703

Improved R-LWE homomorphic masking scheme

Li Zichen[1, 2], Sun Yafei[1], Yang Yatao[1, 3], Liang Lan[1], Cao Guangcan[3]

(1. *College of Communication Engineering*, *Xidian University*, *Xi'an* 710071, *China*; 2. *Beijng Institute of Graphic Communication*, *Beijing* 102600, *China*; 3. *Beijing Electronic Science &Technology Institute*, *Beijing* 100070, *China*)

Abstract: Aiming at the differential power attack of the encryption scheme based on lattice, Reparaz proposed an additively homomorphic R-LWE masking scheme in PQC 2016. This scheme can against the differential power attack effectively, but the additively homomorphic algorithm between the ciphertexts makes the size of noise increase. It declines the rate of decryption correctness. In view of this problem, this paper proposed an improved R-LWE homomorphic masking scheme. By introducing the modular switching technology, it made a modular reduction with the cipher text of additively homomorphic. Under the premising that plaintext and the ciphertext were corresponding, it declined the size of noise in the ciphertext. And it could improve the decryption correctness of the scheme. In order to protect the sub keys, it introduced a the random matrix to mask the sub key. And it makes the correctness analysis and the safety proof. The proposed scheme has better security and efficiency compared to the original scheme.

Key Words: lattice cryptography; R-LWE; side channel defense; mask matrix; modular switch; homomorphic

0　引言

IBM 公司于 2017 年 5 月 17 日宣布成功研制一台拥有 17 个量子位的量子计算处理器，这标志着传统密码面临的挑战越来越严峻。格公钥密码体制是量子环境下安全的密码体系之一，具有很好的密码学性质，受到许多密码学专家的关注。2005 年，Regev 将格理论与学习理论结合在一起，提出了一个格上的新的困难问题——错误学习问题（LWE，Learning with errors）[1]，2010 年 Lyubashevsky 等在欧密会上提出了一种 LWE 的变体 R-LWE（learning with errors over ring）[2]，并同时给出了基于 R-LWE 困难问题的公钥加密方案。但是，现有的基于格密码体制的后量子密码方案也存在侧信道攻击[3]的风险。

文献[4]通过对多项式进行分割，设计一种针对 R-LWE 密码体制的掩码方案，该方案能够有效的抵抗侧信道攻击，但是需要特定的解码器。文献[5]针对文献[4]作出改进，通过分析 R-LWE 的加法同态特性，在解密过程中引入同态的思想，从而改变解密的流程，提高方案的效率，该方案根据同态特性进行解密，不需要特定的解码器，但是，解密正确率有所下降。文献[6]针对高斯取样的实现进行侧信道攻击，并且针对滑动策略的防御措施进行了侧信道攻击。在 CHES 会议上提出的文献[7]，

基金项目：国家自然科学基金资助项目（61370188）

作者简介：李子臣（1965-），男，河南温县人，教授，博士，主要研究方向为密码学、信息安全、数字水印等；孙亚飞（1992-），男，河南内黄人，硕士研究生，主要研究方向为密码学、信息安全（yfsun0112@163.com）；杨亚涛（1978-），男，河南平顶山人，副教授，博士，主要研究方向为无线通信安全、密码学；梁斓（1993-），女，陕西延安人，硕士研究生，主要研究方向为格密码、数字证书；曹广灿（1993-），男，安徽宿州人，硕士研究生，主要研究方向为通信安全、密码学.

利用 Cache 攻击来恢复高斯取样算法的一些输出，从而形成针对格上的签名方案给出了第一个侧信道攻击的方案。文献[8]针对 R-LWE 密码算法的实现设计了一种 8 比特的处理器，使得其能够更加高效的实现加解密过程。文献[9]描述了一种新型的代数编码技术，提出一种简单的随机盲化技术来抵抗计时攻击和能量攻击，并针对高斯取样算法提出一种分割—预计算技术来抵抗侧信道攻击。

本文对文献[5]中的方案进行了深入的分析，指出方案设计中存在的问题：a)解密正确率低；b)未对子密钥进行掩码保护。在原方案的基础上，引入随机矩阵掩码与模数转换技术，通过掩码矩阵对子密钥进行保护，使用模数转换技术降低密文中的噪声尺寸，提高解密正确率。

1　原方案分析

1.1　基础知识

定义 1　设 m 个线性无关的向量 $v_1,\dots,v_m \in R^n$，则一个 m 维满秩格 Λ 定义为向量 $v_1,\dots,v_m$ 的所有整系数线性组合所构成的集合，即 $\Lambda = L(v_1,\dots,v_m) = \{\sum_{i=1}^{m} c_i v_i \mid c_i \in Z\}$，向量 $v_1,\dots,v_m$ 称为格 Λ 的基。

定义 2　错误学习问题（Learning with error，LWE）：已知矩阵 $A \in Z_q^{n\times m}$，向量 $v \in Z_q^n$，向量 e 服从于 Z_q^m 上的概率分布 χ^m，整数 $n,m \ge n, q > 2$。则有：

（1）LWE 判定问题：Z_q^n 与 $v = As + e$ 在计算上是不可区分的，判定向量 v 是均匀取自 Z_q^n，还是由 $v = As + e$ 计算得出。该问题已被证明能够规约到多项式理想格中的近似最短向量问题。

（2）LWE 搜索问题：求出向量 $s \in Z_q^m$，使得其满足 $v = As + e$。

引理 1 假设 p,q 是 2 个奇数，c 是整数向量，c' 是与 $(p/q)c$ 接近的向量且 $c' = c \bmod 2$。对于任意 s，$\| < c,s > \bmod q \| < q/2 - (q/p) l_1(s)$，同时，

$$< c',s > \bmod p = < c,s > \bmod p \bmod 2,$$

且 $$\| < c',s > \bmod p \| < (p/q) \| < c,s > \bmod p \| + l_1(s)$$

其中，$l_1(s)$ 是 s 的 l_1 范数。

该引理表明可在不知密钥的前提下，只需知道密钥长度的界，就可以把密文从一个较大模数转换到一个较小的模数下，且仍可以正确解密。

1.2　原方案回顾

基于 R-LWE 的密码方案主要涉及三个算法：密钥生成算法、加密算法、解密算法。

参数生成：g 为全局已知多项式，n 是多项式环的维度，$p,q,q > p$ 为模数，σ 是离散高斯分布的标准差，e_1,e_2,e_3 是经由离散高斯取样产生的错误向量。

密钥生成算法：从离散高斯分布中取样产生两个多项式 r,s，计算 $p_k = r - g * s$。其中 s 为私钥，p_k 为公钥。

加密算法：首先，对消息进行编码，通过对每比特乘以 $q/2$，将 n 比特输入数据转换为环上的元素 $m \in R_q$。然后计算 $c_1 = g * e_1 + e_2$，$c_2 = p * e_1 + e_3 + m$，输出密文 (c_1, c_2)。

解密算法：接收方收到明文 m 对应的密文 (c_1, c_2)，首先在本地产生随机消息 m_1 并加密产生密文 (c_1', c_2')，其次，对两个密文进行加法运算 $(c_1'', c_2'') = (c_1, c_2) + (c_1', c_2')$，然后，对密文 (c_1'', c_2'') 进行解密运算 $c_1'' s + c_2''$，得明文 $m \oplus m_1$，最后，根据只有解密方拥有的消息 m_1 进行解密，得 $m \oplus m_1 \oplus m_1 = m$。

具体的解密过程如图 1 所示。

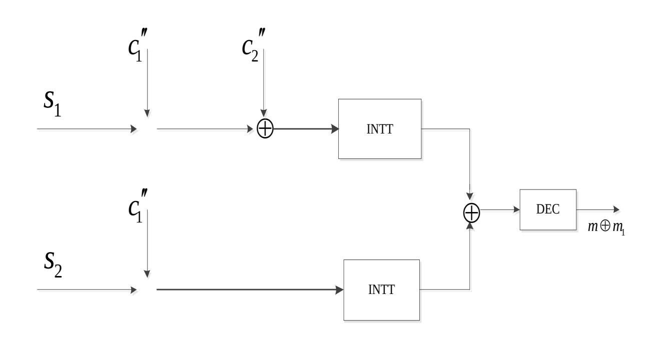


图 1　具有加法同态的 R-LWE 掩码方案

1.3　方案分析

首先，该加法同态解密策略可以看做是对密文的盲化处理，同时，将密钥随机分割为两部分能够使得密钥与密文混合，改变了原有的数据关系，消除了数据之间的依赖性。直观上来讲，该方法能够有效的抵抗一阶差分能量攻击，但是，在软件编程实现时，需要将子密钥载入寄存器进行计算，因此，未加保护的子密钥也是方案的潜在攻击点，攻击者可对子密钥进行恢复，从而获取最终密钥。

其次，由于密文之间的代数相加，造成密文中的噪声尺寸也是代数相加，当噪声尺寸过大，超过解密阈值时，就会出现解密失败的现象。根据文献[5]中的研究结果表明，密文相加使得解密失败率从 3.6×10^{-5} 增加至 3.3×10^{-3}，扩大了将近一百倍。

为了解决上述解密正确率降低的问题，引入模数转换技术，对进行加法运算之后的密文使用模数转换技术，将原模数转换至一个较小的模数，在保证能够正确解密的前提下，降低密文中噪声尺寸的大小，提高了解密正确率。

为了保护子密钥，引入随机掩码矩阵，对子密钥进行掩码处理。使得子密钥处于保护状态，能够有效的避免差分能量攻击。

2　改进的 R-LWE 方案

第 1 章通过分析原始方案，指出其中存在的些许安全隐患，本章针对上述缺陷进行改进，从而提高方案的解密正确率，同时保护子密钥的安全性。方案的密钥生成、加密算法均和原始方案相同。本文只对解密过程进行改进，改进后的解密过程如下所示：

a)解密方接收到明文 m_1 对应的密文 (c_1', c_2')，本地产生随机消息 m_2 并加密得密文 (c_1'', c_2'')，对两个密文进行加法运算，并使用模数规约进行噪声的约减，最终得密文 (c_1, c_2)。计算过程如图 2 所示。

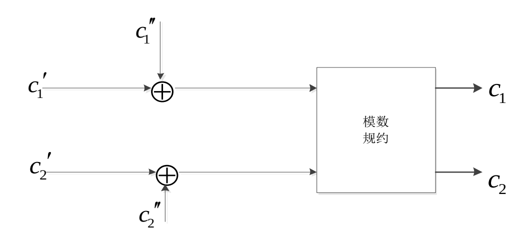


图 2　对密文进行模规约计算

b)用户生成随机矩阵用于对子密钥进行掩码处理。假设生成随机矩阵为 M，计算 $s_1 \oplus M$， $s_2 \oplus M$。

c)在每条分支语句中，根据掩码后的子密钥对密文进行解密计算。分别有 $(s_1 \oplus M)\, e\, c_1 + c_2$， $(s_2 \oplus M)\, e\, c_1$。

d)按照解密规则 $m\% = s \cdot c_1 + c_2$ 进行解密运算，得解密结果 $m_1 \oplus m_2$。

e) 根据本地随机消息 m_2，求得最终原始消息 $m_1 = m_1 \oplus m_2 \oplus m_2$。

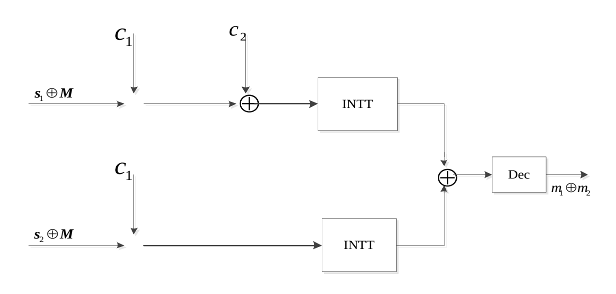


图 3　改进的解密方案

3　方案分析

3.1　正确性分析

正确性证明：为了证明该方案的正确性，首先，验证同态加法的解密正确性， $Dec(c_1, c_2) = Dec(c_1' + c_1'', c_2' + c_2'') = Dec(c_1', c_2') \oplus Dec(c_1'', c_2'') = m_1 \oplus m_2$。

然后，使用 α', α'' 表示 INTT 操作的输出，且 $\alpha = \alpha' + \alpha''$。 α', α'' 分别计算为：

$$\alpha' = \mathrm{INTT}\big((s_1 \oplus M) \cdot c_1 + c_2\big) \tag{1}$$

$$\alpha'' = \mathrm{INTT}\big((s_2 \oplus M) \cdot c_1\big) \tag{2}$$

则

$$\begin{aligned} \alpha &= \mathrm{INTT}(s \cdot c_1 + c_2) = \mathrm{INTT}((s_1 + s_2) \cdot c_1 + c_2) \\ &= \mathrm{INTT}((s_1 \oplus M \oplus M + s_2) \cdot c_1 + c_2) \\ &= \mathrm{INTT}((s_1 \oplus M) \cdot c_1 + c_2 + (s_2 \oplus M) \cdot c_1) \\ &= \mathrm{INTT}((s_1 \oplus M) \cdot c_1 + c_2) + \mathrm{INTT}((s_2 \oplus M) \cdot c_1) \\ &= \alpha' + \alpha'' \end{aligned} \tag{3}$$

最后，对 α 解密可得消息 $Dec(\alpha) = Dec(c_1, c_2) = m_1 \oplus m_2$，则 $m_1 = m_1 \oplus m_2 \oplus m_2$。

3.2　安全性分析

3.2.1 抗计时攻击

计时攻击是根据不同比特位在执行密码算法过程中消耗的时间不同来进行攻击的。根据改进后的密码方案执行流程可知，算法对密钥的处理不是按照原始密钥比特位进行迭代处理的，而是将密钥进行了分割，每个子密钥单独处理，而子密钥的分割是随机进行的，攻击者无法知晓具体的分割方法，也就无法通过计时攻击确认每个子密钥执行的起始点，因此，不能根据计时信息对密钥进行恢复。

3.2.2 抗简单能量攻击

简单能量攻击是对密码算法执行过程中所采集到的能量消耗曲线进行直接分析的技术。本文通过对密钥进行随机分割，改变了原有的计算顺序，攻击者无法确定每个子密钥计算的起始点，也就使得攻击者无法根据能量消耗曲线直观的对密钥进行猜测，从而有效地防止简单能量攻击。

3.2.3 抗差分能量攻击

差分能量攻击主要是根据中间值之间的数据依赖关系进行攻击，只要能够证明数据之间不存在关联，即数据之间的概率分布与密钥无关，就能够有效的抵抗差分能量攻击。

本节通过实现 R-LWE 解密算法，并证明其能够有效的抵抗差分能量攻击。R-LWE 密码算法的解密实现如下所示：

Input : $s_1, s_2, c_1, c_2, M, m_2$
Output : m_1
1. $s_1 \leftarrow s_1 \oplus M$
2. $\alpha' \leftarrow s_1 \cdot c_1$
3. $\alpha' \leftarrow \alpha' + c_2$
4. $\alpha' \leftarrow \mathrm{INTT}(\alpha')$
5. $s_2 \leftarrow s_2 \oplus M$
6. $\alpha'' \leftarrow s_2 \cdot c_1$
7. $\alpha'' \leftarrow \mathrm{INTT}(\alpha'')$
8. $\alpha \leftarrow \alpha' + \alpha''$
9. $m_1 \oplus m_2 \leftarrow Dec(\alpha)$
10. $m_1 \leftarrow m_1 \oplus m_2 \oplus m_2$

定理 1　当矩阵 M，随机消息 m_2 均为 R_q 上的独立均匀分布时，解密算法中的中间变量与敏感信息 s， m_1 服从独立分布。

证明　为了证明上述定理，本文分析每行中变量的分布并且证明所有的中间值与敏感信息 s， m_1 服从独立分布。

第 1,5 行：矩阵 M 是一个随机变量，通过异或运算，使用该变量对中间值进行掩码处理，掩码处理后的变量服从原有的分布，并且不产生任何的敏感信息泄露。

第 2,3,6 行：在 R_q 上， s_1, s_2 服从独立于 s 的分布，并且每条语句的结果都不能用来恢复有关 s 的任何信息。由于 c_2 依赖于密钥 s，但是根据 R-LWE 的假设，攻击者不能通过观察 c_2 获得有关 s 的任何信息。同时， c_1, c_2 是密文的一部分，其中包含随机消息 m_2 对应的密文，因此， c_1, c_2 与密钥 s 和明文消息 m_1 也是相互独立的。

第 4,7 行：相互独立的变量 α', α'' 经过 INTT 转换后仍是相互独立的。

第 8 行：由第 4,7 行可知，两个相互独立的变量相加之后仍然是一个独立的变量，且不泄露任何敏感信息。

第 9 行：输入 α 是经掩码后的数据，因此，该解密结果没有任何的信息泄露。

第 10 行：消息 m_2 是由本地随机产生并保存，通过异或运算可得最终消息 m_1。

综上所述：解密算法中的所有中间变量的分布与敏感信息 s，m_1 相互独立。因此，对于攻击者来说，不能有效的对该算法进行差分能量攻击。

本文设计的掩码防护方案对 R-LWE 算法进行了改进，通过密钥分割技术与同态解密策略，消除了数据与密钥之间的依赖性，能够有效的抵抗计时攻击、简单能量攻击及一阶差分能量攻击和高阶差分能量攻击。

3.3 效率分析

解密正确率分析：文献[5]中指出，由于密文之间的同态加法运算，导致密文中噪声尺寸的增长，一旦噪声尺寸超过阈值，则会出现解密失败的现象。为了避免出现解密失败，本文引入了模数转换技术，通过模数转换，将模数转至一个较小的模数，并能够保证在相同的密钥下解密出正确的消息，这样就能够使得密文中的噪声尺寸降低，从而提高解密正确率。

文献[13]中定理 1 证明了通过模数转换技术，在不知道密钥的值，仅知道密钥的界的前提下，能够将密文转换为一个新的密文，同时模数由原来的模数 q 转换至一个数值较小的模数 p，并且密文对应的明文消息不变。通过该技术降低了密文中的噪声尺寸，能够将噪声大小从 $\|e_q\|$ 降低至 $(p/q)\|e_q\|+1+n\|s\|$，从而提高解密的正确率。

对比分析：功耗平衡技术[11]需要消耗大量的能量，且电路一般都需要重新设计；功耗扰乱技术[12]相比功耗平衡技术能够降低部分能量消耗，但是通常需要大量的数据处理，影响整体性能。对比布尔掩码，布尔掩码需要构建查找表，将所有的可能值都进行存储，加大了存储空间。而本文的同态解密，改变了算法的执行过程，不需要大量的能量开销，仅需要一个用于存储随机消息的寄存器即可。

3.4 对比分析

通过分析对比，本文所提出的方案，比之文献[4]、文献[5]更加安全，增加了对子密钥的保护；效率上通过模数规约能够降低密文中的噪声尺寸，提高解密正确率，从而达到和原始方案相同的解密正确率。对比分析结果如表 1 所示。

表 1 不同方案之间的对比分析

方案	抗侧信道攻击能量	解密正确率	安全性	是否易于实现
文献[4]	√	一般	中	
文献[5]	√	较低	中	√
本文方案	√	高	√	

4 结束语

本文在 Reparaz 等人提出的具有加法同态的 R-LWE 掩码方案基础上，引入模数转换技术，改变密文的处理方式，降低密文中噪声尺寸，提高了解密正确率。通过产生随机掩码矩阵，对子密钥进行掩码处理，使得子密钥得到保护，提高了方案的侧信道防御能力。

参考文献：

[1] Regev O. On lattice, learning with errors, random linear codes, and cryptography [C]// Proc of STOC. 2005: 113-127.

[2] Lyubashevshy V, Peikert C, Regev O. On ideal latice and learning with errors over rings [C]// Proc of Eurocrypt 2010. [S. l.] : Spring-Verlag, 2010: 1-23.

[3] Kocher P, Jaffe J, Jun B. Differential power analysis [C]// Proc of International Cryptology Conference on Advances in Cryptology. [S. l.] : Springer-Verlag, 1999: 388-397.

[4] Reparaz O, Roy S S, Vercauteren F, et al. A masked ring-LWE implementation [C]// Proc of Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2015.

[5] Reparaz O, Clercq R D, Roy S S, et al. Additively homomorphic ring-LWE masking [C]// Proc of Post-Quantum Cryptography. [S. l.] : Springer International Publishing, 2016.

[6] Pessl P. Analyzing the shuffling side-channel countermeasure for lattice-based signatures [C]// Proc of Progress in Cryptology-INDOCRYPT 2016. [S. l.] : Springer International Publishing, 2016.

[7] Bruinderink L G, Hülsing A, Lange T, et al. Flush, Gauss, and reload: a cache attack on the BLISS lattice-based signature scheme [C]// Proc of Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2016.

[8] Liu Z, Seo H, Roy S S, et al. Efficient ring-LWE encryption on 8-bit AVR processors [C]// Proc of Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2015: 663-682.

[9] Saarinen M J O. Arithmetic coding and blinding countermeasures for lattice signatures [J/OL]. Journal of Cryptographic Engineering (2017): 1-14. https://link. springer. com/article/10. 1007/s13389-017-0149-6.

[10] Tong Y, Wang Z, Dai K, et al. A DPA and HO-DPA resistant implementation of AES [J]. Journal of Computer Research & Development, 2009, 46 (3): 377-383.

[11] Burns F, Bystrov A, Koelmans A, et al. Design and security evaluation of balanced 1-of-n circuits [J]. Iet Computers & Digital Techniques, 2012, 6 (2): 125-135.

[12] Liu P C, Chang H C, Lee C Y. A low overhead DPA countermeasure circuit based on ring oscillators [J]. IEEE Trans on Circuits & Systems II Express Briefs, 2010, 57 (7): 546-550.

[13] 汤殿华，祝世雄，王林，等. 基于 RLWE 的全同态加密方案 [J]. 通信学报, 2014, 35 (1): 173-182.